UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/774,169	02/05/2004	Anat Bremler Bar	206,443	7298

7590 04/24/2006

JAY S. CINAMON, ABELMAN, FRAYNE & SCHWAB
150 East 42nd Street
New York, NY 10017

EXAMINER	
NGUYEN, THUONG	

ART UNIT	PAPER NUMBER
2155	

DATE MAILED: 04/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/774,169	BAR ET AL.	
	Examiner	Art Unit	
	Thuong (Tina) T. Nguyen	2155	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 February 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-102* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-102* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 February 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *10/4/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to application 10/774,169 filed 2/5/04. Claims 1-102 are pending and represent method, apparatus, and product for detecting and protecting against worm traffic on a network.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 1, 35 and 69 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. It's unclear to the examiner what are the respective baseline characteristics of the communication traffic? Base on what categories?

4. Claim 3, 37 and 71 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. It's unclear to the examiner what are the amounts of the communication traffic? What are the relatively small amounts of the communication traffic?

5. Claim 16, 50, and 84 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. It's unclear to the examiner what does it

means by "increment the count responsively to each of the data packets responsively to whether among the data packets received previously". To what aspect the applicant compare?

6. Claim 17, 51 and 85 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. It's unclear to the examiner when the count increases? When the source address and the destination address are the same? Or when none of the data packet received previously?

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 1-11, 21-22, 25-45, 55-56, 59-79, 89-90, and 93-102 are rejected under 35 U.S.C. 102(e) as being anticipated by Lyle Patent No. 6,886,102 B1. Lyle teaches the invention as claimed including system and method for protecting a computer network against denial of service attacks (see abstract).

9. As to claim 1, Lyle teaches a method for processing communication traffic, comprising:

monitoring the communication traffic that is directed to a group of addresses on a network (col 5, lines 12-17; Lyle discloses that the method of monitoring the network connection to send and receive information via the network and other computers);

determining respective baseline characteristics of the communication traffic that is directed to each of the addresses in the group (col 8, lines 14-20; Lyle discloses that the method of determined the baseline incident rate and the variance used for all networks);

detecting a deviation from the respective baseline characteristics of the communication traffic directed to at least one of the addresses in the group, wherein the deviation is indicative that at least a portion of the communication traffic is of potentially malicious origin (col 10, lines 28-34; Lyle discloses that the method of detecting the network traffic for the suspicious high volume of network traffic and particular portion of the attacked); and

responsively to detecting the deviation, filtering the communication traffic that is directed to all of the addresses in the group so as to remove at least some of the communication traffic that is of the malicious origin (col 14, lines 26-34; Lyle discloses that the method of analyzed the framework module takes the responsive action to determined to alert the network security administrator and to stop the malicious flow of network traffic).

10. As to claim 2, Lyle teaches the method as recited in claim 1, wherein monitoring the communication traffic comprises selecting a subset of the group of the addresses to monitor responsively to the baseline characteristics (col 8, lines 46-51; Lyle discloses that the method of tracking the network or sub-network which response to the baseline rate).

11. As to claim 3, Lyle teaches the method as recited in claim 2, wherein determining the respective baseline characteristics comprises determining respective amounts of the communication traffic that are directed to the addresses in the group, and wherein selecting the subset comprises selecting the addresses in the subset responsively to the addresses in the subset receiving relatively small amounts of the communication traffic by comparison with other addresses in the group (col 14, lines 56 – col 15, lines 30; Lyle discloses that the method of determined the baseline incident rate for the affected network by a prescribed amount).

12. As to claim 4, Lyle teaches the method as recited in claim 1, wherein the baseline characteristics comprise a distribution of communication protocols used in generating the communication traffic (col 10, lines 19-28; Lyle discloses that the method of tracking the communication traffic using the sniffer module).

13. As to claim 5, Lyle teaches the method as recited in claim 1, wherein the baseline characteristics comprise a distribution of ports to which the communication traffic is directed (col 14, lines 38-42; Lyle discloses that the method of tracking the source of the attack to determined the point of the attack at which the attack is entering the network or sub-network).

14. As to claim 6, Lyle teaches the method as recited in claim 1, wherein the baseline characteristics comprise a distribution of source addresses of the communication traffic (col 14, lines 13-19; Lyle discloses that the method of characteristics of the incident, such as the source address, target address, and preceding characteristics).

15. As to claim 7, Lyle teaches the method as recited in claim 1, wherein the baseline characteristics comprise a distribution of sizes of data packets sent to the addresses in the group (col 10, lines 44-53; Lyle discloses that the method of detecting the particular port for receiving an usually high number of data packets of any type, the sniffer module would identified as the possible attack).

16. As to claim 8, Lyle teaches the method as recited in claim 1, wherein the baseline characteristics are indicative of a distribution of operating systems running on computers that have transmitted the communication traffic (col 21, lines 32-49; Lyle discloses that the method of determined the system of receiving and sending packets).

17. As to claim 9, Lyle teaches the method as recited in claim 8, wherein detecting the deviation comprises reading a Time-To-Live (TTL) field in Internet Protocol headers of data packets sent to the addresses in the group, and detecting a change in values of the TTL field relative to the baseline characteristics (col 11, lines 26-38).

18. As to claim 10, Lyle teaches the method as recited in claim 1, wherein detecting the deviation comprises detecting events that are indicative of a failure in communication between a first computer at one of the addresses in the group and a second computer at another location in the network (col 6, lines 61 – col 7, lines 15 ;

Lyle discloses that the method of tracking the location of the core routers and any associated network element and blocking the potential attack).

19. As to claim 11, Lyle teaches the method as recited in claim 10, wherein detecting the events comprises detecting failures to establish a Transmission Control Protocol (TCP) connection (col 22, lines 25-43).

20. As to claim 21, Lyle teaches the method as recited in claim 1, wherein detecting the deviation comprises detecting a type of the communication traffic that appears to be of the malicious origin, and wherein monitoring the communication traffic comprises collecting specific information relating to the traffic of the detected type (col 4, lines 55-68; Lyle discloses that the method of monitoring the security of the computer network such as suspicious, malicious or virus packets).

21. As to claim 22, Lyle teaches the method as recited in claim 21, wherein collecting the specific information comprises determining one or more source addresses of the traffic of the detected type (col 10, lines 38-43; Lyle discloses that the method of listing the list of suspicious source addresses).

22. As to claim 25, Lyle teaches a method for processing communication traffic, comprising:

monitoring the communication traffic originating from a group of addresses and passing through a selected node on a network (col 12, lines 44-53; Lyle discloses that the method of monitoring the communication traffic of the network for sending and receiving packets);

detecting a pattern in the traffic originating from at least one of the addresses that is indicative of a malicious program running on a computer at the at least one of the addresses (col 13, lines 38-55; Lyle discloses that the method of detecting the network pattern such as monitoring the rate at which the rate for that period of time exceeds by a prescribed amount the average event rate for that particular network or sub-network); and

tracing a route of the traffic from the selected node back to the at least one of the addresses so as to identify a location of the computer on which the malicious program is running (col 6, lines 15-23; Lyle discloses that the method of tracking system of the protected area for the network elements).

23. As to claim 26, Lyle teaches the method as recited in claim 25, wherein tracing the route comprises identifying a port of a switch on the network to which the computer is connected, and comprising disabling the identified port (col 16, lines 54 – col 17, lines 13; Lyle discloses that the method of tracking the port at which the attack was detected to identified the port at which the node through which packets or message associated with the attack entering that node).

24. As to claim 27, Lyle teaches the method as recited in claim 25, wherein detecting the pattern comprises determining that the computer has transmitted packets to a large number of different destination addresses (col 13, lines 9-21; Lyle discloses that the method of detecting the different when sending or receiving messages or packets).

25. As to claim 28, Lyle teaches the method as recited in claim 25, wherein detecting the pattern comprises detecting a large number of packets transmitted by the computer

to a specified port (col 12, lines 63 – col 13, lines 8; Lyle discloses that the method of detecting when the massive numbers of copies of a suspicious but relatively innocuous message in the hope of overloading the security system).

26. As to claim 29, Lyle teaches a method for processing communication traffic, comprising:

monitoring the communication traffic on a network so as to detect packets that are indicative of a communication failure in the network that is characteristic of a worm infection (col 10, lines 53-59; Lyle discloses that the method of monitoring the network traffic for the suspicious in the sense that it indicates that an attack may be taking place);

detecting an increase in a rate of arrival of the packets that are indicative of the communication failure (col 10, lines 60 – col 11, lines 1; Lyle discloses that the method of determined if the rate of certain types of messages exceeds a normal level); and

responsively to the increase, filtering the communication traffic so as to remove at least a portion of the communication traffic that is generated by the worm infection (col 14, lines 26-34; Lyle discloses that the method of analyzed the framework module takes the responsive action to determined to alert the network security administrator and to stop the malicious flow of network traffic).

27. As to claim 30, Lyle teaches the method as recited in claim 29, wherein monitoring the communication traffic comprises detecting Internet Control Message Protocol (ICMP) unreachable packets (col 9, lines 7-37).

28. As to claim 31, Lyle teaches the method as recited in claim 29, wherein monitoring the communication traffic comprises detecting failures to establish a Transmission Control Protocol (TCP) connection (col 22, lines 25-43).

29. As to claim 32, Lyle teaches a method for processing communication traffic, comprising:

monitoring the communication traffic on a network so as to detect ill-formed packets (col 7, lines 9-19; Lyle discloses that the method of scanning the network for the suspicious data within the tracking system);

making a determination, responsively to the ill-formed packets, that at least a portion of the communication traffic has been generated by a worm infection (col 8, lines 26-39; Lyle discloses that the method of determined the alert module for the potential attack); and

responsively to the determination, filtering the communication traffic so as to remove at least the portion of the communication traffic that is generated by the worm infection (col 14, lines 26-34; Lyle discloses that the method of analyzed the framework module takes the responsive action to determined to alert the network security administrator and to stop the malicious flow of network traffic).

30. As to claim 33, Lyle teaches the method as recited in claim 32, wherein the packets comprise a header specifying a communication protocol, and wherein monitoring the communication traffic comprises determining that the packets contain data that are incompatible with the specified communication protocol (col 11, lines 61 –

col 12, lines 19; Lyle discloses that the method of determined the incompatible packet by measure the numerical order of the packet).

31. As to claim 34, Lyle teaches the method as recited in claim 32, wherein the packets comprise a header specifying a packet length, and wherein monitoring the communication traffic comprises determining that the packets contain an amount of data that is incompatible with the specified packet length (col 18, lines 48-59; Lyle discloses that the method of suspicious packet by its bits).

32. As to claim 35, Lyle teaches an apparatus comprising a guard device, which is adapted to

monitor the communication traffic that is directed to a group of addresses on a network (col 5, lines 12-17; Lyle discloses that the apparatus of monitoring the network connection to send and receive information via the network and other computers),

to determine respective baseline characteristics of the communication traffic that is directed to each of the addresses in the group (col 8, lines 14-20; Lyle discloses that the apparatus of determined the baseline incident rate and the variance used for all networks),

to detect a deviation from the respective baseline characteristics of the communication traffic directed to at least one of the addresses in the group, wherein the deviation is indicative that at least a portion of the communication traffic is of potentially malicious origin (col 10, lines 28-34; Lyle discloses that the apparatus of detecting the network traffic for the suspicious high volume of network traffic and particular portion of the attacked), and

responsively to detecting the deviation, to filter the communication traffic that is directed to all of the addresses in the group so as to remove at least some of the communication traffic that is of the malicious origin (col 14, lines 26-34; Lyle discloses that the apparatus of analyzed the framework module takes the responsive action to determined to alert the network security administrator and to stop the malicious flow of network traffic).

33. As to claim 36, Lyle teaches the apparatus as recited in claim 35, wherein the guard device is adapted to select a subset of the group of the addresses to monitor responsively to the baseline characteristics (col 8, lines 46-51; Lyle discloses that the apparatus of tracking the network or sub-network which response to the baseline rate).

34. As to claim 37, Lyle teaches the apparatus as recited in claim 36, wherein the respective baseline characteristics are indicative of respective amounts of the communication traffic that are directed to the addresses in the group, and wherein the guard device is adapted to select the addresses in the subset responsively to the addresses in the subset receiving relatively small amounts of the communication traffic by comparison with other addresses in the group (col 14, lines 56 – col 15, lines 30; Lyle discloses that the apparatus of determined the baseline incident rate for the affected network by a prescribed amount).

35. As to claim 38, Lyle teaches the apparatus as recited in claim 35, wherein the baseline characteristics comprise a distribution of communication protocols used in generating the communication traffic (col 10, lines 19-28; Lyle discloses that the apparatus of tracking the communication traffic using the sniffer module).

36. As to claim 39, Lyle teaches the apparatus as recited in claim 35, wherein the baseline characteristics comprise a distribution of ports to which the communication traffic is directed (col 14, lines 38-42; Lyle discloses that the apparatus of tracking the source of the attack to determined the point of the attack at which the attack is entering the network or sub-network).

37. As to claim 40, Lyle teaches the apparatus as recited in claim 35, wherein the baseline characteristics comprise a distribution of source addresses of the communication traffic (col 14, lines 13-19; Lyle discloses that the apparatus of characteristics of the incident, such as the source address, target address, and preceding characteristics).

38. As to claim 41, Lyle teaches the apparatus as recited in claim 35, wherein the baseline characteristics comprise a distribution of sizes of data packets sent to the addresses in the group (col 10, lines 44-53; Lyle discloses that the apparatus of detecting the particular port for receiving an usually high number of data packets of any type, the sniffer module would identified as the possible attack).

39. As to claim 42, Lyle teaches the apparatus as recited in claim 35, wherein the baseline characteristics are indicative of a distribution of operating systems running on computers that have transmitted the communication traffic (col 21, lines 32-49; Lyle discloses that the apparatus of determined the system of receiving and sending packets).

40. As to claim 43, Lyle teaches the apparatus as recited in claim 42, wherein the guard device is adapted to read a Time-To-Live (TTL) field in Internet Protocol headers

of data packets sent to the addresses in the group, and to detect a change in values of the TTL field relative to the baseline characteristics due to the distribution of the operating systems (col 11, lines 26-38).

41. As to claim 44, Lyle teaches the apparatus as recited in claim 35, wherein the guard device is adapted to detect events that are indicative of a failure in communication between a first computer at one of the addresses in the group and a second computer at another location in the network (col 6, lines 61 – col 7, lines 15 ; Lyle discloses that the apparatus of tracking the location of the core routers and any associated network element and blocking the potential attack).

42. As to claim 45, Lyle teaches the apparatus as recited in claim 44, wherein the events comprise failures to establish a Transmission Control Protocol (TCP) connection (col 22, lines 25-43).

43. As to claim 55, Lyle teaches the apparatus as recited in claim 35, wherein the guard device is adapted to detect a type of the communication traffic that appears to be of the malicious origin, and to monitor the communication traffic so as to collect specific information relating to the traffic of the detected type (col 4, lines 55-68; Lyle discloses that the apparatus of monitoring the security of the computer network such as suspicious, malicious or virus packets).

44. As to claim 56, Lyle teaches the apparatus as recited in claim 55, wherein the specific information comprises one or more source addresses of the traffic of the detected type (col 10, lines 38-43; Lyle discloses that the apparatus of listing the list of suspicious source addresses).

45. As to claim 59, Lyle teaches an apparatus comprising:

monitor the communication traffic originating from a group of addresses and passing through a selected node on a network (col 12, lines 44-53; Lyle discloses that the apparatus of monitoring the communication traffic of the network for sending and receiving packets),

to detect a pattern in the traffic originating from at least one of the addresses that is indicative of a malicious program running on a computer at the at least one of the addresses (col 13, lines 38-55; Lyle discloses that the apparatus of detecting the network pattern such as monitoring the rate at which the rate for that period of time exceeds by a prescribed amount the average event rate for that particular network or sub-network), and

to trace a route of the traffic from the selected node back to the at least one of the addresses so as to identify a location of the computer on which the malicious program is running (col 6, lines 15-23; Lyle discloses that the apparatus of tracking system of the protected area for the network elements).

46. As to claim 60, Lyle teaches the apparatus as recited in claim 59, wherein the guard device is adapted to identify a port of a switch on the network to which the computer is connected, and to instruct the switch to disable the identified port (col 16, lines 54 – col 17, lines 13; Lyle discloses that the apparatus of tracking the port at which the attack was detected to identified the port at which the node through which packets or message associated with the attack entering that node).

47. As to claim 61, Lyle teaches the apparatus as recited in claim 59, wherein the guard device is adapted to detect the pattern by determining that the computer has transmitted packets to a large number of different destination addresses (col 13, lines 9-21; Lyle discloses that the apparatus of detecting the different when sending or receiving messages or packets).

48. As to claim 62, Lyle teaches the apparatus as recited in claim 59, wherein the guard device is adapted to detect the pattern by detecting a large number of packets transmitted by the computer to a specified port (col 12, lines 63 – col 13, lines 8; Lyle discloses that the apparatus of detecting when the massive numbers of copies of a suspicious but relatively innocuous message in the hope of overloading the security system).

49. As to claim 63, Lyle teaches an apparatus comprising:

monitor the communication traffic on a network so as to detect packets that are indicative of a communication failure in the network that is characteristic of a worm infection (col 10, lines 53-59; Lyle discloses that the apparatus of monitoring the network traffic for the suspicious in the sense that it indicates that an attack may be taking place),

to detect an increase in a rate of arrival of the packets that are indicative of the communication failure (col 10, lines 60 – col 11, lines 1; Lyle discloses that the apparatus of determined if the rate of certain types of messages exceeds a normal level), and

responsively to the increase, to filter the communication traffic so as to remove at least a portion of the communication traffic that is generated by the worm infection (col 14, lines 26-34; Lyle discloses that the apparatus of analyzed the framework module takes the responsive action to determined to alert the network security administrator and to stop the malicious flow of network traffic).

50. As to claim 64, Lyle teaches the apparatus as recited in claim 63, wherein the guard device is adapted to detect Internet Control Message Protocol (ICMP) unreachable packets as an indication of the communication failure (col 9, lines 7-37).

51. As to claim 65, Lyle teaches the apparatus as recited in claim 63, wherein the guard device is adapted to detect failures to establish a Transmission Control Protocol (TCP) connection (col 22, lines 25-43).

52. As to claim 66, Lyle teaches an apparatus comprising a guard device, which is adapted:

to monitor the communication traffic on a network so as to detect ill-formed packets (col 7, lines 9-19; Lyle discloses that the apparatus of scanning the network for the suspicious data within the tracking system),

to make a determination, responsively to the ill-formed packets, that at least a portion of the communication traffic has been generated by a worm infection (col 8, lines 26-39; Lyle discloses that the apparatus of determined the alert module for the potential attack), and

responsively to the determination, to filter the communication traffic so as to remove the at least the portion of the communication traffic that is generated by the

worm infection (col 14, lines 26-34; Lyle discloses that the apparatus of analyzed the framework module takes the responsive action to determined to alert the network security administrator and to stop the malicious flow of network traffic).

53. As to claim 67, Lyle teaches the apparatus as recited in claim 66, wherein the packets comprise a header specifying a communication protocol, and wherein the guard device is adapted to detect that the packets contain data that are incompatible with the specified communication protocol (col 11, lines 61 – col 12, lines 19; Lyle discloses that the apparatus of determined the incompatible packet by measure the numerical order of the packet).

54. As to claim 68, Lyle teaches the apparatus as recited in claim 66, wherein the packets comprise a header specifying a packet length, and wherein the guard device is adapted to detect that the packets contain an amount of data that is incompatible with the specified packet length (col 18, lines 48-59; Lyle discloses that the apparatus of suspicious packet by its bits).

55. As to claim 69, Lyle teaches a computer software product, comprising:

a computer-readable medium in which program instructions are stored, which instructions, when read by a computer, cause the computer to monitor communication traffic that is directed to a group of addresses on a network (col 5, lines 12-17; Lyle discloses that the product of monitoring the network connection to send and receive information via the network and other computers),

to determine respective baseline characteristics of the communication traffic that is directed to each of the addresses in the group (col 8, lines 14-20; Lyle discloses that

the product of determined the baseline incident rate and the variance used for all networks),

to detect a deviation from the respective baseline characteristics of the communication traffic directed to at least one of the addresses in the group, wherein the deviation is indicative that at least a portion of the communication traffic is of potentially malicious origin (col 10, lines 28-34; Lyle discloses that the product of detecting the network traffic for the suspicious high volume of network traffic and particular portion of the attacked), and

responsively to detecting the deviation, to filter the communication traffic that is directed to all of the addresses in the group so as to remove at least some of the communication traffic that is of the malicious origin (col 14, lines 26-34; Lyle discloses that the product of analyzed the framework module takes the responsive action to determined to alert the network security administrator and to stop the malicious flow of network traffic).

56. As to claim 70, Lyle teaches the product as recited in claim 69, wherein the instructions cause the computer to select a subset of the group of the addresses to monitor responsively to the baseline characteristics (col 8, lines 46-51; Lyle discloses that the product of tracking the network or sub-network which response to the baseline rate).

57. As to claim 71, Lyle teaches the product as recited in claim 70, wherein the respective baseline characteristics are indicative of respective amounts of the communication traffic that are directed to the addresses in the group, and wherein the

instructions cause the computer to select the addresses in the subset responsively the addresses in the subset receiving relatively small amounts of the communication traffic by comparison with other addresses in the group (col 14, lines 56 – col 15, lines 30; Lyle discloses that the product of determined the baseline incident rate for the affected network by a prescribed amount).

58. As to claim 72, Lyle teaches the product as recited in claim 69, wherein the baseline characteristics comprise a distribution of communication protocols used in generating the communication traffic (col 10, lines 19-28; Lyle discloses that the product of tracking the communication traffic using the sniffer module).

59. As to claim 73, Lyle teaches the product as recited in claim 69, wherein the baseline characteristics comprise a distribution of ports to which the communication traffic is directed (col 14, lines 38-42; Lyle discloses that the product of tracking the source of the attack to determined the point of the attack at which the attack is entering the network or sub-network).

60. As to claim 74, Lyle teaches the product as recited in claim 69, wherein the baseline characteristics comprise a distribution of source addresses of the communication traffic (col 14, lines 13-19; Lyle discloses that the product of characteristics of the incident, such as the source address, target address, and preceding characteristics).

61. As to claim 75, Lyle teaches the product as recited in claim 69, wherein the baseline characteristics comprise a distribution of sizes of data packets sent to the addresses in the group (col 10, lines 44-53; Lyle discloses that the product of detecting

the particular port for receiving an usually high number of data packets of any type, the sniffer module would identified as the possible attack).

62. As to claim 76, Lyle teaches the product as recited in claim 69, wherein the baseline characteristics are indicative of a distribution of operating systems running on computers that have transmitted the communication traffic (col 21, lines 32-49; Lyle discloses that the product of determined the system of receiving and sending packets).

63. As to claim 77, Lyle teaches the product as recited in claim 76, wherein instructions cause the computer to read a Time-To-Live (TTL) field in Internet Protocol headers of data packets sent to the addresses in the group, and to detect a change in values of the TTL field relative to the baseline characteristics due to the distribution of the operating systems (col 11, lines 26-38).

64. As to claim 78, Lyle teaches the product as recited in claim 69, wherein the instructions cause the computer to detect events that are indicative of a failure in communication between a first computer at one of the addresses in the group and a second computer at another location in the network (col 6, lines 61 – col 7, lines 15 ; Lyle discloses that the product of tracking the location of the core routers and any associated network element and blocking the potential attack).

65. As to claim 79, Lyle teaches the product as recited in claim 78, wherein the events comprise failures to establish a Transmission Control Protocol (TCP) connection (col 22, lines 25-43).

66. As to claim 89, Lyle teaches the product as recited in claim 69, wherein the instructions cause the computer to detect a type of the communication traffic that

appears to be of the malicious origin, and to monitor the communication traffic so as to collect specific information relating to the traffic of the detected type (col 4, lines 55-68; Lyle discloses that the product of monitoring the security of the computer network such as suspicious, malicious or virus packets).

67. As to claim 90, Lyle teaches the product as recited in claim 89, wherein the specific information comprises one or more source addresses of the traffic of the detected type (col 10, lines 38-43; Lyle discloses that the product of listing the list of suspicious source addresses).

68. As to claim 93, Lyle teaches a computer software product, comprising:

a computer-readable medium in which program instructions are stored, which instructions, when read by a computer, cause the computer to monitor the communication traffic originating from a group of addresses and passing through a selected node on a network (col 12, lines 44-53; Lyle discloses that the product of monitoring the communication traffic of the network for sending and receiving packets),

to detect a pattern in the traffic originating from at least one of the addresses that is indicative of a malicious program running on a computer at the at least one of the addresses (col 13, lines 38-55; Lyle discloses that the product of detecting the network pattern such as monitoring the rate at which the rate for that period of time exceeds by a prescribed amount the average event rate for that particular network or sub-network), and

to trace a route of the traffic from the selected node back to the at least one of the addresses so as to identify a location of the computer on which the malicious

program is running (col 6, lines 15-23; Lyle discloses that the product of tracking system of the protected area for the network elements).

69. As to claim 94, Lyle teaches the product as recited in claim 93, wherein the instructions cause the computer to identify a port of a switch on the network to which the computer is connected, and to instruct the switch to disable the identified port (col 16, lines 54 – col 17, lines 13; Lyle discloses that the product of tracking the port at which the attack was detected to identified the port at which the node through which packets or message associated with the attack entering that node).

70. As to claim 95, Lyle teaches the product as recited in claim 93, wherein the instructions cause the computer to detect the pattern by determining that the computer has transmitted packets to a large number of different destination addresses (col 13, lines 9-21; Lyle discloses that the product of detecting the different when sending or receiving messages or packets).

71. As to claim 96, Lyle teaches the product as recited in claim 93, wherein the instructions cause the computer to detect the pattern by detecting a large number of packets transmitted by the computer to a specified port (col 12, lines 63 – col 13, lines 8; Lyle discloses that the product of detecting when the massive numbers of copies of a suspicious but relatively innocuous message in the hope of overloading the security system).

72. As to claim 97, Lyle teaches a computer software product, comprising:

a computer-readable medium in which program instructions are stored, which instructions, when read by a computer, cause the computer to monitor the

communication traffic on a network so as to detect packets that are indicative of a communication failure in the network that is characteristic of a worm infection (col 10, lines 53-59; Lyle discloses that the product of monitoring the network traffic for the suspicious in the sense that it indicates that an attack may be taking place),

to detect an increase in a rate of arrival of the packets that are indicative of the communication failure (col 10, lines 60 – col 11, lines 1; Lyle discloses that the product of determined if the rate of certain types of messages exceeds a normal level), and

responsively to the increase, to filter the communication traffic so as to remove at least a portion of the communication traffic that is generated by the worm infection (col 14, lines 26-34; Lyle discloses that the product of analyzed the framework module takes the responsive action to determined to alert the network security administrator and to stop the malicious flow of network traffic).

73. As to claim 98, Lyle teaches the product as recited in claim 97, wherein the instructions cause the computer to detect Internet Control Message Protocol (ICMP) unreachable packets as an indication of the communication failure (col 9, lines 7-37).

74. As to claim 99, Lyle teaches the product as recited in claim 97, wherein the instructions cause the computer to detect failures to establish a Transmission Control Protocol (TCP) connection (col 22, lines 25-43).

75. As to claim 100, Lyle teaches a computer software product, comprising:

a computer-readable medium in which program instructions are stored, which instructions, when read by a computer, cause the computer to monitor the communication traffic on a network so as to detect ill-formed packets (col 7, lines 9-19;

Lyle discloses that the product of scanning the network for the suspicious data within the tracking system),

to make a determination, responsively to the ill-formed packets, that at least a portion of the communication traffic has been generated by a worm infection (col 8, lines 26-39; Lyle discloses that the product of determined the alert module for the potential attack), and

responsively to the determination, to filter the communication traffic so as to remove the at least the portion of the communication traffic that is generated by the worm infection (col 14, lines 26-34; Lyle discloses that the product of analyzed the framework module takes the responsive action to determined to alert the network security administrator and to stop the malicious flow of network traffic).

76. As to claim 101, Lyle teaches the product as recited in claim 100, wherein the packets comprise a header specifying a communication protocol, and wherein the instructions cause the computer to detect that the packets contain data that are incompatible with the specified communication protocol (col 11, lines 61 – col 12, lines 19; Lyle discloses that the product of determined the incompatible packet by measure the numerical order of the packet).

77. As to claim 102, Lyle teaches the product as recited in claim 100, wherein the packets comprise a header specifying a packet length, and wherein the instructions cause the computer to detect that the packets contain an amount of data that is incompatible with the specified packet length (col 18, lines 48-59; Lyle discloses that the product of suspicious packet by its bits).

Claim Rejections - 35 USC § 103

78. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

79. Claims 12-13, 46-47, and 80-81 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lyle, Patent No. 6,886,102 B1 in view of Porras, Patent No. 6,321,338 B1.

Lyle teaches the invention substantially as claimed including system and method for protecting a computer network against denial of service attacks (see abstract).

80. As to claim 12, Lyle teaches the method as recited in claim 1. But Lyle fails to teach the claim limitation wherein receiving packets that are indicative of a communication failure in the network that is characteristic of a worm infection, and wherein filtering the communication traffic comprises deciding to filter the communication traffic responsively to receiving the packets.

However, Porras teaches network surveillance (see abstract). Porras teaches the limitation wherein receiving packets that are indicative of a communication failure in the network that is characteristic of a worm infection, and wherein filtering the communication traffic comprises deciding to filter the communication traffic responsively to receiving the packets (col 9, lines 49-63).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Lyle in view of Porras so that the engine could filter out the unwanted packets. One would be motivated to do so to prevent the potential attack and ensure the liability of the network.

81. As to claim 13, Lyle teaches the method as recited in claim 12. But Lyle fails to teach the claim limitation wherein receiving the packets comprises receiving Internet Control Message Protocol (ICMP) unreachable packets.

However, Porras teaches the limitation wherein receiving the packets comprises receiving Internet Control Message Protocol (ICMP) unreachable packets (col 5, lines 4-29).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Lyle in view of Porras so that filtering out the ICMP packets, which reach the gateway. One would be motivated to do so to ensure the ill-formed packet will not travel into the network.

82. As to claim 46, Lyle teaches the apparatus as recited in claim 35. But Lyle fails to teach the claim limitation wherein the guard device is adapted to receive packets that are indicative of a communication failure in the network that is characteristic of a worm infection, and to decide to filter the communication traffic responsively to receiving the packets.

However, Porras teaches the limitation wherein the guard device is adapted to receive packets that are indicative of a communication failure in the network that is

characteristic of a worm infection, and to decide to filter the communication traffic responsively to receiving the packets (col 9, lines 49-63).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Lyle in view of Porras so that the engine could filter out the unwanted packets. One would be motivated to do so to prevent the potential attack and ensure the liability of the network.

83. As to claim 47, Lyle teaches the apparatus as recited in claim 46. But Lyle fails to teach the claim limitation wherein the packets comprise Internet Control Message Protocol (ICMP) unreachable packets.

However, Porras teaches the limitation wherein the packets comprise Internet Control Message Protocol (ICMP) unreachable packets (col 5, lines 4-29).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Lyle in view of Porras so that filtering out the ICMP packets, which reach the gateway. One would be motivated to do so to ensure the ill-formed packet will not travel into the network.

84. As to claim 80, Lyle teaches the product as recited in claim 69. But Lyle fails to teach the claim limitation wherein the instructions cause the computer to receive packets that are indicative of a communication failure in the network that is characteristic of a worm infection, and to decide to filter the communication traffic responsively to receiving the packets.

However, Porras teaches the limitation wherein the instructions cause the computer to receive packets that are indicative of a communication failure in the

network that is characteristic of a worm infection, and to decide to filter the communication traffic responsively to receiving the packets (col 9, lines 49-63).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Lyle in view of Porras so that the engine could filter out the unwanted packets. One would be motivated to do so to prevent the potential attack and ensure the liability of the network.

85. As to claim 81, Lyle teaches the product as recited in claim 80. But Lyle fails to teach the claim limitation wherein the packets comprise Internet Control Message Protocol (ICMP) unreachable packets.

However, Porras teaches the limitation wherein the packets comprise Internet Control Message Protocol (ICMP) unreachable packets (col 5, lines 4-29).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Lyle in view of Porras so that filtering out the ICMP packets, which reach the gateway. One would be motivated to do so to ensure the ill-formed packet will not travel into the network.

86. Claims 14-20, 23-24, 48-54, 57-58, 82-88, and 91-92 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lyle, Patent No. 6,886,102 B1 in view of Trcka, Patent No. 2001/0039579 A1.

Lyle teaches the invention substantially as claimed including system and method for protecting a computer network against denial of service attack (see abstract).

87. As to claim 14, Lyle teaches the method as recited in claim 1. But Lyle fails to teach the claim limitation wherein monitoring the communication traffic comprises making a determination that one or more packets transmitted over the network are ill-formed, and wherein filtering the communication traffic comprises deciding to filter the communication traffic responsively to the ill-formed packets.

However, Trcka teaches network security and surveillance system (see abstract). Trcka teaches the limitation wherein monitoring the communication traffic comprises making a determination that one or more packets transmitted over the network are ill-formed, and wherein filtering the communication traffic comprises deciding to filter the communication traffic responsively to the ill-formed packets (page 4, paragraph 41).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Lyle in view of Trcka so that the system would filter out the malicious packet. One would be motivated to do so to ensure the safety of the network form the virus and hacker.

88. As to claim 15, Lyle teaches the method as recited in claim 1. But Lyle fails to teach the claim limitation wherein detecting the deviation comprises incrementing a count of events that are indicative of the malicious origin of the communication traffic, and deciding whether to filter the communication traffic responsively to the count.

However, Trcka teaches the limitation wherein detecting the deviation comprises incrementing a count of events that are indicative of the malicious origin of the communication traffic, and deciding whether to filter the communication traffic responsively to the count (page 7, paragraph 79; page 8, paragraph 80).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Lyle in view of Trcka so that the system could enabling/disabling packet filtering. One would be motivated to do so to records the data-link level traffic without interfering with the normal flow of traffic.

89. As to claim 16, Lyle teaches the method as recited in claim 15, wherein detecting the deviation comprises receiving data packets of potentially malicious origin, each data packet having a respective source address and destination address, and wherein incrementing the count comprises determining an amount by which to increment the count responsively to each of the data packets responsively to whether among the data packets received previously, responsively to which the count was incremented, at least one data packet had the same respective source address and at least one data packet had the same respective destination address (col 7, lines 38-49; col 19, lines 51 – col 20, lines 23; Lyle discloses that the method of identified the messages related to a known or suspected attack or possibility that an attack is taking place).

90. As to claim 17, Lyle teaches the method as recited in claim 16, wherein determining the amount by which to increment the count comprises incrementing the count only if none of the data packets received previously, responsively to which the count was incremented, had at least one of the same respective source address and the same respective destination address (col 15, lines 48 – col 16, lines 6; Lyle discloses that the method of tracking back to the point of attack at which the attack entered the network or sub-network).

91. As to claim 18, Lyle teaches the method as recited in claim 1. But Lyle fails to teach the claim limitation wherein detecting the deviation comprises detecting a type of the communication traffic that appears to be of the malicious origin, and wherein filtering the communication traffic comprises intercepting the communication traffic of the detected type.

However, Trcka teaches the limitation wherein detecting the deviation comprises detecting a type of the communication traffic that appears to be of the malicious origin, and wherein filtering the communication traffic comprises intercepting the communication traffic of the detected type (figure 3).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Lyle in view of Trcka so that filtering the suspicious packet. One would be motivated to do so to ensure the safety of the network.

92. As to claim 19, Lyle teaches the method as recited in claim 18, wherein detecting the type comprises determining at least one of a communication protocol and a port that is characteristic of the communication traffic (col 5, lines 34-44; Lyle discloses that the method of managing the exchange of information between network elements located at different physical locations via external connections such as an Internet connection).

93. As to claim 20, Lyle teaches the method as recited in claim 18, wherein detecting the type comprises determining one or more source addresses of the communication traffic that appears to be of the malicious origin, and intercepting the communication traffic sent from the one or more source addresses (col 16, lines 44-49; Lyle discloses

that the method of tracking the source of an attack to determine the point of attack at which it is entering the network or sub-network).

94. As to claim 23, Lyle teaches the method as recited in claim 1. But Lyle fails to teach the claim limitation wherein monitoring and filtering the communication traffic comprise monitoring and filtering the communication traffic that is transmitted into a protected area of the network containing the group of the addresses so as to exclude the communication traffic from the area.

However, Trcka teaches the limitation wherein monitoring and filtering the communication traffic comprise monitoring and filtering the communication traffic that is transmitted into a protected area of the network containing the group of the addresses so as to exclude the communication traffic from the area (figure 5).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Lyle in view of Trcka so that filtering the suspicious packet, which tries to enter through the protected area. One would be motivated to do so to improves the network security.

95. As to claim 24, Lyle teaches the method as recited in claim 23, and comprising monitoring the communication traffic that is transmitted by computers in the protected area so as to detect an infection of one or more of the computers by a malicious program (col 10, lines 35-38; Lyle discloses that the method of tracking the system interconnect across the network, such as a private network which is a protected area).

96. As to claim 48, Lyle teaches the apparatus as recited in claim 35. But Lyle fails to teach the claim limitation wherein the guard device is adapted to make a

determination that one or more packets transmitted over the network are ill-formed, and to decide to filter the communication traffic responsively to the ill-formed packets.

However, Trcka teaches the limitation wherein the guard device is adapted to make a determination that one or more packets transmitted over the network are ill-formed, and to decide to filter the communication traffic responsively to the ill-formed packets (page 4, paragraph 41).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Lyle in view of Trcka so that the system would filter out the malicious packet. One would be motivated to do so to ensure the safety of the network form the virus and hacker.

97. As to claim 49, Lyle teaches the apparatus as recited in claim 35. But Lyle fails to teach the claim limitation wherein the guard device is adapted to increment a count of events that are indicative of the malicious origin of the communication traffic, and to decide whether to filter the communication traffic responsively to the count.

However, Trcka teaches the limitation wherein the guard device is adapted to increment a count of events that are indicative of the malicious origin of the communication traffic, and to decide whether to filter the communication traffic responsively to the count (page 7, paragraph 79; page 8, paragraph 80).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Lyle in view of Trcka so that the system could enabling/disabling packet filtering. One would be motivated to do so to records the data-link level traffic without interfering with the normal flow of traffic.

98. As to claim 50, Lyle teaches the apparatus as recited in claim 49, wherein the guard device is coupled to receive data packets of potentially malicious origin, each data packet having a respective source address and destination address, and is adapted to determine an amount by which to increment the count responsively to each of the data packets responsively to whether among the data packets received previously, responsively to which the count was incremented, at least one data packet had the same respective source address and at least one data packet had the same respective destination address (col 7, lines 38-49; col 19, lines 51 – col 20, lines 23; Lyle discloses that the apparatus of identified the messages related to a known or suspected attack or possibility that an attack is taking place).

99. As to claim 51, Lyle teaches the apparatus as recited in claim 40, wherein the guard device is adapted to increment the count only if none of the data packets received previously, responsively to which the count was incremented, had at least one of the same respective source address and the same respective destination address (col 15, lines 48 – col 16, lines 6; Lyle discloses that the apparatus of tracking back to the point of attack at which the attack entered the network or sub-network).

100. As to claim 52, Lyle teaches the apparatus as recited in claim 35. But Lyle fails to teach the claim limitation wherein the guard device is adapted to detect a type of the communication traffic that appears to be of the malicious origin, and to filter the communication traffic by intercepting the communication traffic of the detected type.

However, Trcka teaches the limitation wherein the guard device is adapted to detect a type of the communication traffic that appears to be of the malicious origin, and

to filter the communication traffic by intercepting the communication traffic of the detected type (figure 3).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Lyle in view of Trcka so that filtering the suspicious packet. One would be motivated to do so to ensure the safety of the network.

101. As to claim 53, Lyle teaches the apparatus as recited in claim 52, wherein the type of the communication traffic that appears to be of the malicious origin is characterized by at least one of a communication protocol and a port (col 5, lines 34-44; Lyle discloses that the apparatus of managing the exchange of information between network elements located at different physical locations via external connections such as an Internet connection).

102. As to claim 54, Lyle teaches the apparatus as recited in claim 52, wherein the guard device is adapted to determine one or more source addresses of the communication traffic that appears to be of the malicious origin, and to intercept the communication traffic sent from the one or more source addresses (col 16, lines 44-49; Lyle discloses that the apparatus of tracking the source of an attack to determine the point of attack at which it is entering the network or sub-network).

103. As to claim 57, Lyle teaches the apparatus as recited in claim 35. But Lyle fails to teach the claim limitation wherein the guard device is adapted to monitor and filter the communication traffic that is transmitted into a protected area of the network containing the group of the addresses so as to exclude the communication traffic from the area.

However, Trcka teaches the limitation wherein the guard device is adapted to monitor and filter the communication traffic that is transmitted into a protected area of the network containing the group of the addresses so as to exclude the communication traffic from the area (figure 5).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Lyle in view of Trcka so that filtering the suspicious packet, which tries to enter through the protected area. One would be motivated to do so to improves the network security.

104. As to claim 58, Lyle teaches the apparatus as recited in claim 57, wherein the guard device is adapted to monitor the communication traffic that is transmitted by computers in the protected area so as to detect an infection of one or more of the computers by a malicious program (col 10, lines 35-38; Lyle discloses that the apparatus of tracking the system interconnect across the network, such as a private network which is a protected area).

105. As to claim 82, Lyle teaches the product as recited in claim 69. But Lyle fails to teach the claim limitation wherein the instructions cause the computer to make a determination that one or more packets transmitted over the network are ill-formed, and to decide to filter the communication traffic responsively to the ill-formed packets.

However, Trcka teaches the limitation wherein the instructions cause the computer to make a determination that one or more packets transmitted over the network are ill-formed, and to decide to filter the communication traffic responsively to the ill-formed packets (page 4, paragraph 41).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Lyle in view of Trcka so that the system would filter out the malicious packet. One would be motivated to do so to ensure the safety of the network form the virus and hacker.

106. As to claim 83, Lyle teaches the product as recited in claim 69. But Lyle fails to teach the claim limitation wherein the instructions cause the computer to increment a count of events that are indicative of the malicious origin of the communication traffic, and to decide whether to filter the communication traffic responsively to the count.

However, Trcka teaches the limitation wherein the instructions cause the computer to increment a count of events that are indicative of the malicious origin of the communication traffic, and to decide whether to filter the communication traffic responsively to the count (page 7, paragraph 79; page 8, paragraph 80).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Lyle in view of Trcka so that the system could enabling/disabling packet filtering. One would be motivated to do so to records the data-link level traffic without interfering with the normal flow of traffic.

107. As to claim 84, Lyle teaches the product as recited in claim 83, wherein when the computer is coupled to receive data packets of potentially malicious origin, each data packet having a respective source address and destination address, the instructions cause the computer to determine an amount by which to increment the count responsively to each of the data packets responsively to whether among the data packets received previously, responsively to which the count was incremented, at least

one data packet had the same respective source address and at least one data packet had the same respective destination address (col 7, lines 38-49; col 19, lines 51 – col 20, lines 23; Lyle discloses that the product of identified the messages related to a known or suspected attack or possibility that an attack is taking place).

108. As to claim 85, Lyle teaches the product as recited in claim 84, wherein the instructions cause the computer to increment the count only if none of the data packets received previously, responsively to which the count was incremented, had at least one of the same respective source address and the same respective destination address (col 15, lines 48 – col 16, lines 6; Lyle discloses that the product of tracking back to the point of attack at which the attack entered the network or sub-network).

109. As to claim 86, Lyle teaches the product as recited in claim 69. But Lyle fails to teach the claim limitation wherein the instructions cause the computer to detect a type of the communication traffic that appears to be of the malicious origin, and to filter the communication traffic by intercepting the communication traffic of the detected type.

However, Trcka teaches the limitation wherein the instructions cause the computer to detect a type of the communication traffic that appears to be of the malicious origin, and to filter the communication traffic by intercepting the communication traffic of the detected type (figure 3).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Lyle in view of Trcka so that filtering the suspicious packet. One would be motivated to do so to ensure the safety of the network.

110. As to claim 87, Lyle teaches the product as recited in claim 86, wherein the type of the communication traffic that appears to be of the malicious origin is characterized by at least one of a communication protocol and a port (col 5, lines 34-44; Lyle discloses that the product of managing the exchange of information between network elements located at different physical locations via external connections such as an Internet connection).

111. As to claim 88, Lyle teaches the product as recited in claim 86, wherein the instructions cause the computer to determine one or more source addresses of the communication traffic that appears to be of the malicious origin, and to intercept the communication traffic sent from the one or more source addresses (col 16, lines 44-49; Lyle discloses that the product of tracking the source of an attack to determine the point of attack at which it is entering the network or sub-network).

112. As to claim 91, Lyle teaches the product as recited in claim 69. But Lyle fails to teach the claim limitation wherein the instructions cause the computer to monitor and filter the communication traffic that is transmitted into a protected area of the network containing the group of the addresses so as to exclude the communication traffic from the area.

However, Trcka teaches the limitation wherein the instructions cause the computer to monitor and filter the communication traffic that is transmitted into a protected area of the network containing the group of the addresses so as to exclude the communication traffic from the area (figure 5).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Lyle in view of Trcka so that filtering the suspicious packet, which tries to enter through the protected area. One would be motivated to do so to improves the network security.

113. As to claim 92, Lyle teaches the product as recited in claim 91, wherein the instructions cause the computer to monitor the communication traffic that is transmitted by computers in the protected area so as to detect an infection of one or more of the computers by a malicious program (col 10, lines 35-38; Lyle discloses that the product of tracking the system interconnect across the network, such as a private network which is a protected area).

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thuong (Tina) Nguyen whose telephone number is 571-272-3864, and the fax number is 571-273-3864. The examiner can normally be reached on 8:00 AM-5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Saleh Najjar can be reached on 571-272-4006. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Thuong (Tina) Nguyen
Patent Examiner/Art Unit 2155

SALEH NAJJAR
SUPERVISORY PATENT EXAMINER